Первицкая Ирина Сергеевна
студентка
Стерлитамакский филиал ФГБОУ ВО «Башкирский государственный университет»
г. Стерлитамак, Республика Башкортостан

DOI 10.21661/r-553553

ПРАВОВЫЕ ОСНОВЫ ИСПОЛЬЗОВАНИЯ СОВРЕМЕННЫХ ЦИФРОВЫХ ТЕХНОЛОГИЙ В РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ В РОССИЙСКОЙ ФЕДЕРАЦИИ

Аннотация: *в статье рассмотрен материал, раскрывающий сущность цифровых технологий, которые применяются в практике расследования преступлений следователями и криминалистами. Приведены примеры таких технологий. Дана оценка совершенным преступлениям с использованием цифровых технологий. Описана правовая база использования современных цифровых технологий. Сделан вывод, ждут ли изменения нормативно-правовую базу с точки зрения расширения перечня актов, а также углубления в какие-либо нюансы термина «цифровые технологии». Приведены примеры, касательно подготовки следователей к работе с современными цифровыми технологиями.*

Ключевые слова*: цифровые технологии, глобальная цифровизация, цифровая информация, расследование преступлений, криминальная среда, цифровые следы преступлений, электронные носители информации, нормативно-правовая база.*

Если начать изучать всю мировую историю с момента становления государственности, то можно сделать вывод о том, что на протяжении всего периода осуществлялись накопление, хранение, обработка и использование информации различного плана, о разных объектах и в разных целях. При этом сразвитием научно-технического прогресса совершенствовались технологии по совершению таких операций. Логично, что с внедрением в повседневную жизнедеятельность цифровых технологий закономерным стало использование их возможностей во всех сферах жизни общества.

Таким образом, целесообразно дать толкование понятию «цифровые технологии». Итак, под «цифровыми технологиями» понимаются такие технологии, которые используют компьютеры, а также любую другую современную технику для записи кодовых импульсов и сигналов в определенной последовательности и с определенной частотой [1]. Основными видами цифровых технологий, согласно перечню ведущих направлений, развития и использования данных считаются интернет вещей; большие данные (Big Data); машинное обучение и искусственный интеллект.

Совершенно предсказуем тот момент, что в условиях глобальной цифровизации эффективность предупреждения, выявления, раскрытия и расследования преступлений находится в прямо пропорциональной зависимости от того, какими возможностями о работе со следственно-значимой информацией обладают правоохранительные органы.

На сегодняшний день активно используются следующие технологии при раскрытии ирасследовании преступлений: «Мобильный криминалист»; МСР-ТВ; Система «Папилон»; Система «Портрет-Поиск»; Следопыт-М; «Big data»; «Deep learning»; «FindFace security»; «Гран-УД»; «СТРАС-СК»; цифровая звуко-фото- видеосъемка; дроны; устройство «Сфера»; комплекс «Скарабей».

Доктор юридических наук, Аминев Ф.Г., считает целесообразным использование системы криминалистической регистрации, а также базы данныхДНК-профилей биологического материала человека в ближайшей перспективе для того, чтобы повысить эффективность борьбы с преступностью [2, с. 11–12].

Однако не только свершение научно-технической революции послужило толчком к активному использованию инновационных цифровых технологий в органах правопорядка. Так же, по оценкам и российских и зарубежных ученых, приходится наблюдать нарастающие темпы использования этих технологий в криминальной среде [3, с. 9–12]. В качестве примеров можно привести сбыт наркотических веществ, хищение денежных средств в кредитных организациях, посягательства на жизнь человека, безопасность государства (например,

террористические организации используют сеть Интернет для набора единомышленников в свои ряды, а также занимаются вербованием).

Прирост числа данных преступлений, который фиксируется в двукратном размере в течение нескольких лет подряд, наглядно показывает, что эта проблема стала одной из главных угроз экономической безопасности Российской Федерации.

Таким образом, противодействие преступлениям с использованием цифровых технологий – это приоритетное направление деятельности органов внутренних дел, что неоднократно подчеркивалось в решениях коллегии МВД России.

Говоря об основных направлениях в деятельности органов внутренних дел, необходимо также отметить такую важную сторону государственной политики в сфере противодействия указанным преступлениям, как совершенствование уголовно-процессуального законодательства. При этом оно должно соответствовать следующему требованию: уголовно-процессуальной форме стоит адекватно отражать содержание правоохранительной деятельности о борьбе высокотехнологичной преступностью.

Но не стоит забывать и о нравственных основах деятельности следователей и криминалистов, которые при применении цифровых технологий в уголовном процессе должны гарантировать минимизацию рисков ущемления прав и законных интересов участников уголовного судопроизводства.

Исходя из сказанного, остро назрел вопрос создания соответствующей нормативно-правовой базы, а также пересмотра некоторых федеральных законов путем внесения необходимых поправок. К наиболее значимым документам, касательно регулирования цифрового пространства, можно отнести следующие:

1. Прогноз научно-технологического развития Российской Федерации напериод до 2030 года от 3 января 2014 г [4]. В данном прогнозе описано одно из перспективных направлений научного исследования, такого как информационная безопасность, которая включает методы и средства биометрической идентификации личности; противодействие новым вызовам информационной войны и киберпреступности в ИКТ.

2. Стратегия научно-технологического развития Российской Федерации от 1 декабря 2016 г. №642 [5]. В ней в качестве одной из приоритетных задач является противодействие терроризму и идеологическому экстремизму, а также киберугрозам и иным источникам опасности для общества, экономики и государства.

3. Стратегия развития отрасли информационных технологий РФ на 2014–2020 годы и на перспективу до 2025 года от 1 ноября 2013 года №2036-р [6]. В качестве основных задач выступают обеспечение информационной безопасности; широкомасштабное открытие государственных баз данных; развитие электронного документооборота; развитие центров обработки и хранения информации. Все это также способствует своевременному раскрытию и расследованию преступлений.

4. Государственная программа «Информационное общество» от 31 марта 2020 г. №386–20 [7]. Данная программа содержит ряд подпрограмм. Одной из них является «Безопасность в информационном обществе», к задачам которой относится противодействие распространению идеологии терроризма, экстремизма и пропаганды насилия. Также в подпрограмме «Информационное государство» задачами являются повышение надежности и защиты государственных информационных систем и сервисов; сохранение ретроспективной архивной информации и перевод ее в электронный вид для эффективного использования в интересах государства, общества и граждан. Иными словами, указанная программа защищает следственно-значимые данные от посторонних посягательств. В свою очередь, это повышает эффективность расследования преступлений.

5. Отдельные статьи Уголовного кодекса Российской Федерации от 13 июня 1996 г. №63-ФЗ в редакции от 30 декабря 2020 г. [8]. В законе напрямую не дается определение «цифровых технологий» и не предложена их классификация. Однако упоминаются такие термины, как компьютерная информация; вредоносные компьютерные программы; специальные технические средства, предназначенные для негласного получения информации; информационно-телекоммуникационные устройства.

6. Отдельные статьи Уголовно-процессуального кодекса РоссийскойФедерации от 18 декабря 2001 г. №174-ФЗ в редакции от 24 февраля 2021 г. [9]. В УПК упоминаются технологии видеоконференцсвязи, СМС-сообщения, электронный документооборот, технологии видеозаписи, аудиозаписи, съемки, видеонаблюдения.

7. Федеральный закон «Об оперативно-розыскной деятельности» от 12 августа 1995 г. №144-ФЗ в редакции от 2 августа 2019 г. [10]. Данный закон устанавливает возможность получения значимой информации не только в устной или текстовой форме, но и в форме видео- или аудиозаписи, фотоизображения, компьютерных файлов.

8. Федеральный закон «О полиции» от 7 февраля 2011 г. №3-ФЗ в редакции от 24 февраля 2021 г. [11]. Статья 11 указывает на порядок использования достижений науки и техники, современных технологий и информационных систем в деятельности органов правопорядка.

Необходимо отметить тот факт, что указанная нормативно-правовая база не будет выступать в качестве исчерпывающего перечня, имеющего свою значимость для практики раскрытия и расследования преступлений. На сегодняшний день законодатель разрабатывает поэтапную разработку и реализации инициатив, которые направлены, в свою очередь на снятие первостепенных барьеров, препятствующих развитию цифрового пространства.

Одновременно с этим планируется работа над такими концептуальными актами, которые могли бы создать возможности для установления максимально эффективной системы управления изменениями. Такая система должна включать регуляторные песочницы, площадки для технологического и организационного апробирования современных цифровых технологий.

Также те методы и средства, которые включены в состав цифровой криминалистики, активно используются в деятельности Следственного комитета РФ [12, с. 126–133]. Например, проводятся следственные действия с осмотром и изъятием компьютеров, мобильных телефонов и устройств, электронных носителей информации (флеш-карты, жесткие диски, внешние жесткие диски, дискеты,

карты памяти, CD/DVD диски) с участием сотрудников Главного управления криминалистики. Далее уже такое оборудование подлежит осмотру в целях изъятия необходимой информации для раскрытия преступления о горячим следам.

Стоит отметить, что в связи с постоянно увеличивающимся количеством цифровых технологий возникла потребность в обучении специалистов всем нюансам использования новой информации в доказывании, а также стало проводиться целевое обучение студентов со специализацией в сфере исследования цифровой информации в Московском государственном техническом университете имени Н.Э. Баумана.

Обобщая вышесказанное, можно сделать вывод о том, что все перечисленные мероприятия – это гарантия того, что достижения цифровой криминалистики будут и далее эффективно использоваться следственными органами в раскрытии и расследовании преступлений. Также будет изменяться законодательная база в том темпе, в котором будут создаваться и внедряться в следственную и криминалистическую деятельность новые цифровые технологии.

Список литературы

1. Словарь-справочник терминов нормативно-технической документации от 2015г.: словари [Электронный ресурс]. Режим доступа: http://www.find-info.ru/doc/dictionary/normative-technical-documentation/index-214.htm#214 (дата обращения: 26.02.202).

2. Аминев Ф.Г. Об организационном аспекте современной технологии всеобщей ДНК-регистрации граждан / Ф.Г. Аминев, В.А. Анисимов // Правовое государство: теория и практика. – 2020. – №2(60). – С. 11–12.

3. Гриб В.Г. Криминалистика и цифровые технологии / В.Г. Гриб, И.О. Тюнис // Российский следователь. – 2019. – №4. – С. 9–12.

4. Прогноз научно-технологического развития Российской Федерации на период до 2030 года, утвержденный Правительством РФ от 3 января 2014 г [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_157978/ (дата обращения: 27.02.2021).

5. Стратегия научно-технологического развития Российской Федерации, утвержденную Указом Президента РФ от 1 декабря 2016 г. №642 [Электронный ресурс]. – Режим доступа: https://sudact.ru/law/ukaz-prezidenta-rf-ot-01122016-n-642/strategiia-nauchno-tekhnologicheskogo-razvitiia-rossiiskoi-federatsii/ (дата обращения: 28.02.2021).

6. Стратегия развития отрасли информационных технологий РФ на 2014-2020 годы и на перспективу до 2025 года, утвержденную распоряжением Правительства РФ от 1 ноября 2013 года №2036-р [Электронный ресурс]. – Режим доступа: https://digital.gov.ru/common/upload/Strategiya_razvitiya_otrasli_IT_2014–2020_2025.pdf (дата обращения: 28.02.2021).

7. Государственная программа «Информационное общество», утвержденная в новой редакции постановлением Правительства РФ от 31 марта 2020г. №386–20 [Электронный ресурс]. – Режим доступа: https://www.garant.ru/products/ipo/prime/doc/73759938/ (дата обращения: 01.03.2021).

8. Уголовный кодекс Российской Федерации от 13 июня 1996г. №63-ФЗ в редакции от 30 декабря 2020г [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_10699/ (дата обращения: 01.03.2021).

9. Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001г. №174-ФЗ в редакции от 24 февраля 2021г. [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_34481/ (дата обращения: 01.03.2021).

10. Федеральный закон «Об оперативно-розыскной деятельности» от 12 августа 1995г. №144-ФЗ в редакции от 2 августа 2019г [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_7519/ (дата обращения: 01.03.2021).

11. Федеральный закон «О полиции» от 07 февраля 2011г. №3-ФЗ в редакции от 24 февраля 2021г [Электронный ресурс]. – Режим доступа:

http://www.consultant.ru/document/cons_doc_LAW_110165/ (дата обращения: 01.03.2021).

12. Серебренникова А.В. Цифровая криминалистика и ее значение для расследования преступлений / А.В. Серебренникова // INTERNATIONAL LAW JOURNAL. – 2019. – №4(2). – С. 126–133.